African Journal of Advanced Pure and Applied Sciences (AJAPAS)
Online ISSN: 2957-644X
Volume 5, Issue 3, 2026
Page No: 448-457
Website: *https://aaasjournals.com/index.php/ajapas/index*
ISI 2025: 1.126 **SJIFactor 2024: 6.752** **معامل التأثير العربي: 1.62**

Behavioral cybersecurity: An Evaluation study of insecure Banking data storage practices on smartphones (A Field study on Libyan bank customers)

Ababaker Mohamed Noureldeen [1 *], Khalifah Salem Masoud [2]
[1,2] Department of Computer Technology, Higher Institute of Sciences and Technology – Tamezawa, Brack, Libya

الأمن السيبراني السلوكي: دراسة تقيميه لممارسات التخزين غير الرسمي للبيانات المصرفية على الهواتف الذكية (دراسة ميدانية على عملاء المصارف الليبية)

أبوبكر محمد نورالدين [1*]، خليفة سالم مسعود [2]
[2,1] قسم تقنيات الحاسب، المعهد العالي للعلوم والتقنية تامزاوة الشاطئ، براك، ليبيا

[*]*Corresponding author: tandrd2010@gmail.com*

Received: June 19, 2026	Accepted: September 12, 2026	Published: September 22, 2026

Abstract:
This study presents a methodology for assessing the level of security awareness among users of banking applications in Libya regarding the risks of insecurely storing sensitive banking data on their smart devices. It focuses particularly on a common practice among many customers: storing their banking data, such as account numbers, passwords, or even IP addresses, in their contacts or photo albums under pseudonyms or their real names. This practice is widespread among many customers, exposing this data to serious risks. The study employed a descriptive and analytical approach, utilizing an electronic questionnaire distributed to a sample of 255 respondents from various Libyan banks. The data was then processed using the open-source Jamovi software for statistical analysis. The results showed a significant increase in the prevalence of insecure data storage behavior among a large segment of the sample. The variable (P1, saving data in the contacts list) recorded the lowest mean score at 1.49, with 77% reporting a consistent or recurring practice of this behavior. Inferential tests (T-test) and ANOVA revealed no statistically significant differences based on gender, age group, or educational level, indicating that this behavior is generally widespread across all groups. The results also revealed a lack of understanding among customers regarding the risks associated with application permissions and automatic cloud synchronization, making them vulnerable to cyberattacks and hacking.
The study concluded with several recommendations for banks, including developing encrypted vaults within banking applications to eliminate the need for customers to store their data in other applications not designed for sensitive banking information. It also recommended conducting awareness campaigns to highlight the dangers of this behavior. Furthermore, the study recommended that customers use biometric authentication systems as an alternative to traditional passwords or PINs.

Keywords: Behavioral cybersecurity, banking applications, insecure storage, cognitive laziness.

الملخص
تقدم هده الدراسة منهجية لتقيم مستوى الوعي الامني لدى مستخدمي التطبيقات المصرفية في ليبيا لمخاطر التخزين غير الآمن للبيانات المصرفية الحساسة على أجهزتهم الذكية حيث تركز بشكل خاص على سلوك متبع لدى عديد من العملاء وهو تخرين بياناتهم المصرفية من أرقام حساباتهم أو كلمات المرور او حتى أرقام IPN في سجل جهات الاتصال CONTACTS أو في معرص الصور بأسماء مستعارة او صريحة حيث تعتبر هده الممارسات شائعة لذي العديد من العملاء ما يعرض هده البيانات لمخاطر جسيمة.

واعتمدنا في الدراسة على نهج الوصفي والتحليلي، استخدمنا الاستبيان الالكتروني حيت وزع على عينة فعلية مكونة من 255 مستجيبا من زبائن عدد من مصارف ليبية مختلفة، حيت ثمت معالجة البيانات بواسطة برنامج Jamovi مفتوح المصدر للتحليل الإحصائي. اظهرت النتائج ارتفاعا ملحوظ في نسب انتشار سلوك التخزين العير الامن لدى شريحة واسعة من العينة حيث سجل المتغير (P1 الحفظ في سجل جهات الاتصال Contact) أدنى متوسط حسابي بلغ (1.49) ونسنه ممارسة دائمة او متكررة لهذا السلوك 77% كما بينت الاختبارات الاستدلالية (T-Test) والاخبار(ANOVA) عن عدم وجود فروقات ذات دلالة إحصائية بحسب الجنس او الفئات العمرية او المستوى التعليمي ما يفيد بأن هذا السلوك منتشر بشكل عام بين جميع الفئات، واظهرت النتائج بوجود عدم فهم لذى العملاء بخطورة اذونات التطبيقات و كذلك المزامنة السحابية التلقائية، مما يجعلهم عرضة للهجمات السيبرانية والاختراق .
وخلصت الدراسة بجملة من التوصيات للمصارف بتطوير خزنات مشفرة داخل التطبيقات المصرفية تغنى العملاء من تخرين بياناتهم في تطبيقات أخرى غير مصممة لحفظ البيانات المصرفية الحساسة وكذلك القيام بحملات توعوية توضح خطورة هذا السلوك، وخلصت الدراسة أيضا بجملة من التوصيات للعملاء باستخدام أنظمة المصادقة البيو مترية (Biometric Authentication System) كبديل لكلمات المرور التقليدية او الأرقام السرية.

الكلمات المفتاحية: الأمن السيبراني السلوكي، التطبيقات المصرفية، التخزين غير الامن، الكسل المعرفي.

المقدمة

يعتر أمن المعلومات احد اهم المحاور الأساسية في التحول الرقمي ما جعل المؤسسات تولى اهتمام كبير بأمن وسلامة معلوماتها وفى السنوات الأخيرة شهدة ليبيا نقلة نوعية و تطور في مجال الرقمة وبالأخص المصارف[1]، ما ترتب عنة تغير سريع في كيفه تعامل العملاء مع حساباتهم المصرفية اذ أصبحت التطبيقات المصرفية جزا أساسي يمس معاملاتهم اليومية وإدارة معاملاتهم البنكية من تحويل أموال والاطلاع على الأرصدة[2] ، وقد رافق هذا التحول تطور كبير في مجال التشفير وامن المعلومات اذ تتعرص الأنظمة المرتبطة بشكة الأنترنت لهجمات سيبرانية وقرصنة إلكترونية تهدد سلامتها وتعطل عملها على مستوى المصارف عالميا[3]، وتأكد العدد من الدراسات ان العنصر البشري يعتبر هو الحلقة الأضعف والتحدي الأبرز في سلسلة الأمن السيبراني ومن هذا المنطلق جاءت الدراسات لتسليط الضوء على التحديات التي تواجه المصارف في ليبيا حيت أوضحت تحديات تقنية عديدة ويعتبر عامل الوعى بالأمن السيبراني لذى العنصر البشرى ابرز تحدياتها ويمتل نقطة الضعف في دورة امن المعلومات [4].على الرغم من الجهود التي تبدلها المصارف في تأمين تطبيقاتها وتوعية عملائها الا انه لاتزال هناك مشكلة أساسية قائمة تتمثل في ميل عدد كبير من مستخدمي التطبيقات المصرفية منح الأولوية لسرعة الوصول لخدمات التطبيقات على حساب الامن التقني .

رغم المساعي التي نبدلها المصارف للحفاظ على امن وسلامة خدماتها الالكترونية، غير ان هناك تحديا حقيقي يكمن في ان مستخدمي التطبيقات المصرفية يفضلون سهولة الاستخدام والوصول السريع للبيانات بدلا من اتباع اساليب أمنة لحفظ البيانات، حيت يلجا العملاء لاستخدام أساليب تقنية بدائية غير أمنه. على سبيل المثال تخزين البيانات المصرفية في قائمة جهات الاتصال بهواتفهم الذكية تحت أسماء مستعارة أو أسماء حقيقية. حيث تكمن المشكلة الرئيسة المرتبط بهذا السلوك أن بعض التطبيقات غير مصممة لتكون آمنة لحفظ بيانات حساسة[5]، ولا تستطيع حماية المعلومات ما يعرض هذه البيانات لخطر الاختراق ويجعل العملاء أهدافًا سهلة لأي هجوم إلكتروني. تتسبب هذه الممارسات غير السليمة تقنيا مخاطر عديدة التي قد يجهلها معظم المستخدمين، ناهيك عن انتهاك خصوصية البيانات الناتجة عن أذونات لوصول إلى قائمة جهات الاتصال الخاصة بهم للتطبيقات خارجية[6]، وكذلك تخزين البيانات على خوادم سحابية التي تقوم بالمزامنة التلقائية مثل جهات اتصال ووسائط التخزين على الهاتف من هذا المنطلق، تسلط دراستنا الضوء على ظاهرة التخزين غير الرسمي للبيانات من جانب ثقني، تهدف للإجابة على سؤالها: الرئيسي ما هو مستوى وعي العملاء بالمشاكل السيبرانية المرتبطة بتخزين البيانات المصرفية على هواتفهم وقياس مدى أنتشاره ومدى تأثير هذا الوعي على ممارساتهم اليومية؟ .

كما تهدف لدراسة تأثير المتغيرات الديموغرافية (مثل الجنس والفئة العمرية والمؤهلات التعليمية) على الالتزام بإجراءات الأمن السيبراني، كما تهدف ايضا الكشف عن الدوافع التي تدفع العملاء إلى تبني هذه الممارسات الخطيرة. ولتحقيق أهداف الدراسة تستند إلى عدد من الفرضيات، أولها أن التخزين غير الرسمي للبيانات المصرفية الحساسة منتشر بشكل كبير بين المستخدمين، وأن عدم وجود بدائل سهلة الاستخدام ضمن التطبيقات المصرفية يُعدّ دافعًا رئيسيًا وراء هذه الممارسة. ومن الفرضيات عدم وجود فهم لذا العملاء بمخاطر أذونات التطبيقات ومزامنة البيانات السحابية. تتقاطع هذه الدراسة مع العديد من الدراسات التي تناولتها الابحاث السابقة التي تناولت مفهوم الوعى الأمني الدي يعكس مدى فهم الفرد للمخاطر[7]، والتي تعرف بالثغرات الأمنية والتي فيها يقوم المستخدم بتخزين البيانات في تطبيقات غير مصممة لهدا الغرض[8] [9]. اضف الى ذلك فجوة النية والسلوك حيت أن الوعي بالمخاطر لا يمنع بالضرورة من أرتكبها ما يعرف بالكسل المعرفي[10]، وقد ظهرت بعض الأبحاث في هذا المجال ان المستخدمين احيانا يفضلون سهولة الوصول الى البيانات على حساب امن البيانات وسلامتها وان زيادة التعقيدات الامنية قد يحفر المستخدم لتخزين البيانات بطريقة خطرة

[11] [12]. يتوافق هدا الرأي مع الدراسات التي تشير الى ان سهولة استخدام واجهات التطبيقات الذكية قللت الفروقات الديمغرافية التي تعرض المستخدم للمخاطر ولم تعد المؤهلات التعليمية توفر الحماية من مخاطر السلوكيات الخاطئة [14][13]. بل ان هدة التهديدات تستهدف نقاط الضعف السلوكية والنفسية [15] ، وعلى الصعيد المحلى والاقليمي كشفت دراسة قامت بها الجمعية العربية للأمن السيبراني ان 61%من المستخدمين يجهلون كيفية عمل اذونات المزامنة للتطبيقات بينما قام 43%منهم بتخزين بيانات حساسة بتنسيقات مختلفة على هواتفهم[16] .

من استعراض الادبيات السابقة تتبين فجوه تتمثل في ندرة الدراسات التي تناولت التخزين الغير الرسمي كظاهرة سلوكية مستقلة حيث ركزة اغلب الدراسات السابقة على الهجمات الخارجية مثل التصيد والاحتيال متجاهلة التهديد الداخلي الناتج عن المستخدم نفسة ،ولذلك تكتسب دراستنا اهمية خاصة لتطبيقها على السياق المحلى الدى يواجه تحديا تقنيا ومعرفيا حيث يعتبر التحول الرقمي في القطاع المصرفي حديثا نسبيا ،مع تركيزها على ممارسات سلوكية خاطئة هي "تخزين البيانات المصرفية الحساسة في سجل جهات الاتصال أو معرض الصور" .حيث تهدف دراستنا الى تزويد إدارات تقنية المعلومات في المصارف الليبية بأدوات ونتائج ميدانية تسهم في تصمم سياسات تقنية وتوعوية للحد من الاحتيال المالي الناتج عن الخطأ البشري .

منهجية البحث

اعتمدنا على المنهج الوصفي التحليلي لوصف سلوكيات البشرية بدقة وتحليلها، يتيح هدا المنهج وصف وملاحظة الظاهرة كما في الواقع وتفسير ابعادها واسبابها دون التأثير على متغيراتها.

العينة ومجتمع البحث

تتكون عينة الدراسة من عدد من زبائن المصارف الليبية مختلفة ولهم حسابات نشطة ويستخدمون التطبيقات المصرفية المنصبة على هواتفهم الذكية بانتظام، حيث ثم اعتماد عينة عشوائية لضمان تمثيل مختلف الفئات العمرية والمستويات التعليمية ،ونظرا لكبر حجم المجتمع وصعوبة تحديد العدد الإجمالي لزبائن المصارف وكذلك نظرا لطبيعة الدراسة التي تركز على سلوكيات معينة فقد ثم الاعتماد على عينة ميسرة مكونة من 225 مستجوبا،ويعتبر هذا العدد كافيا احصائيا لأغراض هدة الدراسة،مع وجود 3 قيم مفقودة في متغيرات الممارسة (القيم المفقودة =3) مما ينتج حجم عينة فعلية قدرها (N=222).

أداة جمع البيانات

قمنا بتوظيف أداة الاستبيان وذك للاختبار فرضيات البحث ولجمع البيانات ثم نطور الاستبيان ونشر إلكترونيا وذلك للوصول لأكبر عدد من المستجوبين وللتغلب على العوائق الجغرافية، حيث تم مراعات المعاير التالية الداعمة لعملية جمع البيانات واستخلاص النتائج الإحصائية.

- الموثوقية وسلامة محتوى الاستبيان: حيث تم التأكد من صحته من قبل خبير في امن المعلومات والسلوك.
- الثبات: ثم اختباره باستخدام معامل ألفا كرونباخ والذي بلغ 0.83 وهو مستوى ثبات عالي.

وقد تم تطوير الاستبيان بناء على مراجعة ادبيات الدراسات السابقة المتعلقة بأمن السيبراني السلوكي وتم تقسيمة الى ثلاثة محاور رئيسية:

- القسم الأول (البيانات الأساسية والديموغرافية) يهدف هذا القسم للتعرف على الخصائص العامة لأفراد العينة والتي ستستخدم لقياس الفروق الإحصائية ومدا تأثيرها على السلوك الأمني للمستخدم.
- القسم التانئ (ممارسات تخزين البيانات المصرفية) يتضمن هذا القسم عناصر محددة لقياس تكرار سلوكيان التخزين الغير رسمي للبيانات المصرفية الحساسة على الهواتف الذكية مثل (الاحتفاظ بأرقام الحسابات والأرقام السرية في سجل جهات الاتصال، استخدام الأسماء المستعارة، الاحتفاظ بصور ارقام الحسابات أو الارقام السرية أو صور البطاقات المصرفية في معرض الصور في الهاتف او في تطبيق مدون الملاحظات).
- القسم الثالث (الدوافع والتدابير السلوكية) تم إنشاء هذا القسم لاكتشاف الأسباب العملية والسلوكية النفسية التي تدفع العملاء لتبني ممارسات التخزين الغير الامن متل سهولة الاسترجاع، كثرة الحسابات، عدم القدرة على تذكر الأرقام أو نقص الوعي المعرفي.

المتغيرات الرئيسة للدراسة

جدول (1) يوضح المتغيرات الرئيسة قيد الدراسة

المتغير	الوصف
P1	حفظ ارقام الحسابات وارقام البطاقات في سجل الاتصال
P2	حفظ ارقام (PIN) السرية تحت اسماء مستعارة او صريحة
P3	الاحتفاظ بصور البطاقات او ارقام الحسابات في تطبيق معرض الصور
P4	كتابة بيانات تسجيل الدخول للحساب في تطبيق الملاحظات على الهاتف

النتائج والمناقشة

التحليل الاحصائي والأساليب المستخدمة

اعتمدنا برنامج Jamoviللتحليل الإحصائي الذي يعتبر من البرامج مفتوحة المصدر في هذا المجال تمت دراسات الاحصاء الوصفي لقياس التكرارات والنسب المئوية وحساب المتوسطات الحسابية والانحرافات المعيارية واختبار (t-test) للعينات المستقلة واختبار (Independent Samples t-test _Welch's) لقياس الفروقات حسب الجنس وفحصها وتم استخدام تحليل التباين الأحادي (Welch's — ANOVA One-Way) لفحص الفروق بحسب العمر والمستوى التعليمي. ومعامل ارتباط سبيرمان: لقياس طبيعة العلاقة بين المستوى التعليمي وسلوك التخزين غير الآمن واستخدمنا الانحدار اللوجستي (Logistic Regression) لتحديد أقوى النسب الإحصائية بممارسة التخزين غير الرسمي.

الخصائص الديمغرافية للعينة الدراسة

الفئات العمرية

جدول (2): التوزيعات التكرارية للفئات العمرية (N=225)

العمر Age	التكرارCounts	النسبة المئوية%	النسبة المئويةCumulative % التراكمية
1 (18 –30)	34.0	15.1%	15.1%
2 (31 – 45)	74.0	32.9%	48.0%
3 (45 – 60)	85.0	37.8%	85.8%
4(Over 60 years)	32.0	14.2%	100.0%

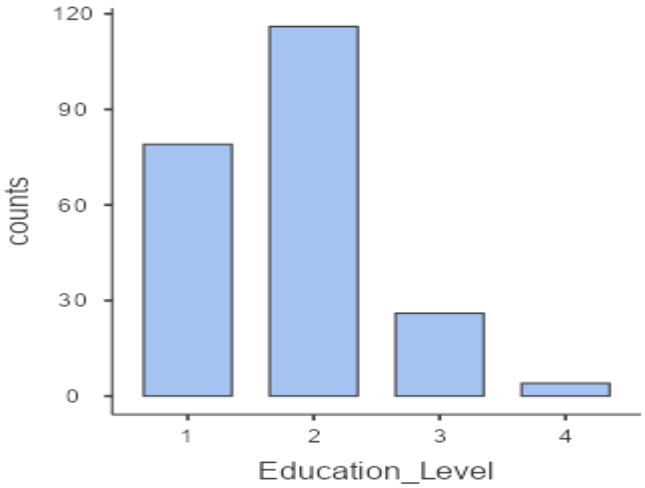
استأثرت الفئة العمرية من (45-60 سنة) بأعلى نسبة تمثيل حيت بلغت تسبه التمثيل 37.8% (85 مبحوثا) وتعتبر هذه الفئة الاكثر تعامل مع التطبيقات المصرفية ،تم جاءت الفئة (31-45) بنسبة 32.9% (74 مبحوثا) تم تليها الفئة العمرية (18-30 سنة)بنسبة تمثيل 15,1% (34 مبحوثا) في حين لم تتجاور الفئة العمرية (اكبر من 60 سنة) نسبة 14% ، ويفيد هذا التوريع بان العينة تعكس شريحة البالغين الدين يمثلون القاعدة العريضة لمستخدمي التطبيقات المصرفية.

التوزيع وفق المستوى التعليمي

جدول (3): التوريع التكراري للفئات وفق المستو التعليمي

المستوى التعليمي Education Level	التكرارCounts	النسبة المئوية%	%النسبة المئوية التراكمية Cumulative
1 High school or less (ثانوي او اقل)	799.00	35.1%	35.1%
2University/Bachelor's degree(جامعي)	116.00	51.6%	86.7%
3 Master's degree (دراسات عليا)	26.00	11.6%	98.2%
4 Ph.D.(دكتوراه)	4.00	1.8%	100.0%

اظهر التوزيع حسب المستوى التعليمي للعينة ان السبة الاكبر من المستجوبين من حاملي درجة البكالوريوس بنسبة 51.1 % (116 مبحوثا) ثم يليهم حاملو المستوى الثانوي او افل بنسبة 35.1 % (79مبحوثا) فيما لم تتجاوز نسبة حاملي الدراسات العليا مجتمعة نسبة 13.5% من أجمالي العينة.



شكل (1): توزيع افراد العينة وفقا لمتغير المستوى التعليمي.

الإحصاء الوصفي لمتغيرات التخزين غير الرسمي للبيانات

استخدمنا مقياس ليكرث الرباعي (1=دائما ،2=أحيانا ،3=نادرا،4=ابدا) لقياس معدل السلوك ومن المهم ملاحظة ان اتجاه المقياس يعكس علاقة عكسية حيت يشير المتوسط المنخفض الى ارتفاع معدل انتشار تكرار ممارسات تخزين غيز امنة، بينما يشبر المتوسطات العالية أي درجة من الوعي وسلوك منضبط.

جدول (4): المقاييس الوصفية لمتغيرات التخزين غير آمن للعينة: (N=222)

Indicator	P1(Contacts App)	P2 (Pseudonymous PIN)	p3 (Gallery)	p4 (Notes App)
N	222	222	222	222
Missing	3	3	3	3
Mean	1.91	2.22	2.21	3.09
Median	2.00	2.00	2.00	4.00
Standard deviation	0.935	1.03	1.17	1.16
Minimum	1	1	1	1
Maximum	4	4	4	4

تحليل المتغير (P1) الحفظ الحفظ في تطبيق جهات الاتصال

جدول (5) التوريع التكراري الاجابات العينة على متغير السلوك (P1) الحفظ في تطبيق جهات الاتصال

خيارات الاجابة	التكرار(Counts)	النسبة المئوية%	النسبة التراكمية (Cumulative %)
1(دائما)	90.0	40.5%	40.5%
2(احيانا)	81.0	36.5%	77.0%
3(نادرا)	33.0	14.9%	91.9%
4(ابدا)	18.0	8.1%	100.0%

سجل المتغير P1لممارسة سلوك الحفظ في تطبيق جهات الاتصال أدني متوسط حسابي بين كل المتغيرات هذا ما جعلة الاكثر شيوعا في مجتمع العينة، وتوضح النسبة التراكمية ان 77% من المستخدمين يمارسون هذا السلوك بانتظام ما يجعله سلوك عالي الخطورة بسبب سهولة وصول تطبيقات التي منحت صلاحية الوصول لجهات الاتصال.

تحليل المتغير (P2) استخدام الأسماء المستعارة في حفظ الأرقام السرية ورموز PIN

جدول (6): التوزيع التكراري لإجابات العينة على سلوك الحفظ بأسماء مستعارة

خيارات الاجابة	التكرار (Counts)	%النسبة المئوية	النسبة التراكمية (Cumulative %)
1(دائما)	58.0	26.1%	26.1%
2(احيانا)	98.0	44.1%	70.3%
3(نادرا)	25.0	11.3%	81.5%
4(ابدا)	41.0	18.5%	100.0%

يتضح من متوسط الممارسات عند 22.2 سلوك متوسط الانتشار ومتوسط الخطورة حيث تتركز النسبة الأكبر في الخيار (أحيانا) بنسبة (41.1%) بينما بلغة نسبة الممارسات (دائما , أحيانا) الكلية (70.3%) ما يوضح ان المستخدمين يعتمدون على سلوك التمويه للمعلومات ما يعتبر سلوك بدائي للحفظ الامن للبيانات.

تحليل المتغير(P3) لسلوك الحفظ في تطبيق مغرض الصور Gallery

جدول (7): التوزيع التكراري الاجابات على السلوك الحفظ في تطبيق معرض الصور

خيارات الاجابة	التكرار (Counts)	%النسبة المئوية	النسبة التراكمية (Cumulative %)
1(دائما)	80.0	36.0%	36.0%
2(احيانا)	68.0	30.6%	66.7%
3(نادرا)	22.0	9.9%	76.6%
4(ابدا)	52.0	23.4%	100.0%

جاء المتغير P3 في المرتبة الثالثة بحسب درجة الخطورة والانتشار بين المستخدمين بمتوسط 2.21 حيث ان نسبة قدرها(36.0%) منهم يقوم بهذا السلوك دائما وتصل نسبة الممارسة الاجمالية 66.7 % يمارسون هذا السلوك دائما او أحيانا وتكمن خطورة هذا السلوك في تعرض البيانات الساكنة (Data at rest) لثغرة المزامنة التلقائية وصلاحيات الوصول لمعرض الصور التي تطلبها بعض التطبيقات.

تحليل المتغير(P3) لسلوك الحفظ في تطبيق الملاحظات

جدول (8): التوزيع التكراري الاجابات على السلوك الحفظ في تطبيق الملاحظات

خيارات الاجابة	التكرار (Counts)	%النسبة المئوية	النسبة التراكمية (Cumulative %)
1(دائما)	36.0	16.2%	16.2%
2(احيانا)	32.0	14.4%	30.6%
3(نادرا)	31.0	14.0%	44.6%
4(ابدا)	123.0	55.4%	100.0%

اظهر هذا المتغير مسار اكثر أمانا من المتغيرات السابقة حيث سجل متوسط حسابي(3.09) وقيمة وسيط قدرها 4.00 حيث يمتنع اكثر من تصف العينة (55.4%) عن ممارسة هذا السلوك وتصل نسبة الامتناع الكلى والجزئي الى (69.4 %) ما يجعل الامتناع السلوك الأكثر أمنا، وبالبحث عن الأسباب الكامنة وراء هذا الامتناع وجدا ان السبب الرئيسي هو ان جزء كبير من المستخدمون يفتقر المعرفة بوجود تطبيق الملاحظات،وبعضهم لا يستخدمه أصلا ما اخرجة عن نطاق ممارستهم اليومية ومع ذلك فان نسبة (31.0%) من افراد العينة يمارسون هذا اسلوك(دائما ,احيانا) يجعله تهديا سيبراني لا يمكن تجاهله.

الإحصاء الاستدلالي تحليل الفروق.

لاختبار الدلالة الإحصائية والاختلافات في أجمالي ممارسات التخزين الغير الآمن للبيانات اعتمدنا اختبار (T-test(Welch's) للعينات المستقلة ،حيث تكم ميزة هذا الاختبار في عدم اشتراطه وجود تجاس التباين بين المجموعات بما يضمن موثوقية النتائج وتحصلنا على النتائج التالة:

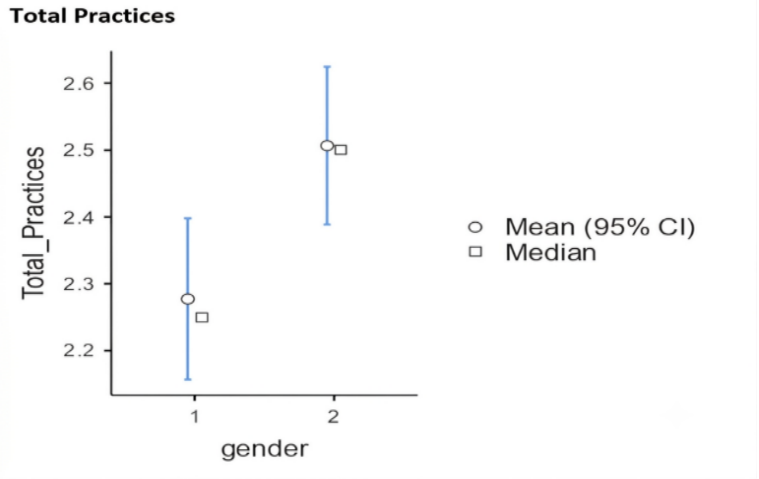
تحليل الفرق حسب الجنس.

جدول (9): نتائج اختبار ((T-test(Welch's للفروق ممارسات التخزين غير الرسمي وفقا لمتغير الجنس

	الاختبار	قيمة الاختبار(Statistic)	درجة الحرية(df)	مستوى الدلالة(p)
أجمالي الممارسات	Welch's t	-1.28	177	0.205

Note. H_a $\mu_1 \neq \mu_2$

وجود القيمة (t=-128) عند (df=177) وقيمة الاحتمالية (p=0.205> 0.05) تدعم الفرضية الصفرية لا توجد فروقات ذات دلالة إحصائية في ممارسة هدا السلوك بين الذكور والانات ما يجعله سلوك شائع بين الجنسين ويرجع دلك لتفافة استخدام عامة.



شكل :(2) فروق ممارسات التخزين غير الرسمي بين الجنسين في المصارف الليبية

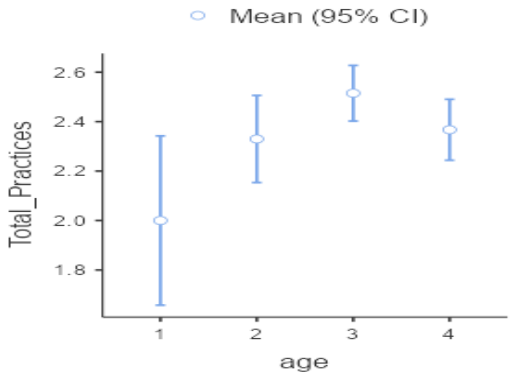
تحليل الفروق في أجمالي ممارسات التخزين الغير الآمن وفقا لمتغير الفئة العمرية

للتحقق مما إذا كانت هناك اختلافات ذات دلالة إحصائية في ممارسات التخزين الغير رسمية ترتبط بالمتغير الديمغرافي للفئات العمرية تم اعتماد تحليل التباين الأحادي الاتجاه (one-way ANOVA test) يعد هدا الاختبار الخيار المنهجي الأكثر دقه للتعامل مع البيانات الغير متساوية بين المجموعات وأحجام العينة الفرعية المختلفة وتحصلنا على النتائج التالية:

جدول (10): نتائج اختبار تحليل التباين احادي الاتجاه (one-way ANOVA (Welch's للفروق في ممارسات التخزين الغير رسمي للبيانات حسب الفة العمرية

	(F) قيمة الاختبار	(df1) درجة الحرية	(df2) درجة الحرية المعدلة	(P) احتمالية
أجمالي الممارسات	1.08	3	44.4	0.369

اوضحت نتائج اختبار ANOVA ان قيمة F بلغت1.08 عند درجتي حرية (3, 44.4) بقيمة احتمالية (P=0.360) تتجاوز الدالة (α=0.05) وعلى هذا الاساس لا توجد فروق ذات دلالة إحصائية بين هده الفئات العمرية المختلفة ما يشير الى ان هذه الممارسات عامة لا تقتصر على فئة بعينها لتشمل مختلف المراحل العمرية ما يؤكد ضرورة لتوعية شامله غير مخصصة لفئه عمرية محددة.



شكل(3): يوضح الاختلافات في ممارسات التخزين وفقا للفئات العمرية.

تحليل التاين الاحادى (ANOVA) للفروق وفق المستوى التعليمي

لاختبار مدى تاثير المستوى التعليمي على مجمل الممارسات التخزين الغير رسمي وفق للأختبار (one-way ANOVA Welch's)) تحصلنا على النتائج التالية:

جدول (11): نتائج اختبار تحليل التباين احادي الاتجاه (one-way ANOVA (Welch's) للفروق في ممارسات التخزين الغير رسمي للبيانات حسب المستوى التعليمي

	قيمة الاختبار (F)	درجة الحرية (df1)	درجة الحرية المعدلة (df2)	احتمالية (P)
أجمالي الممارسات	1.23	3	10.8	0.347

تشير نتيجة الاختبار الى عدم وجود اى فروقات ذات دلالة إحصائية وفق متغير المستوى التعليمى حيت بلغة قيمة الاختبار 1.38 ومستوى الدلالة P=0.347 متجاوزة مستوى الدالة المعتمدة (α=0.05) ما يشير احصائيا الى عدم وجود فروق في ممارسات التخزين الغير رسمي للبيانت بين مختلف المستويات التعليمية.

تعد هده النتيجة من ابرز النتائج في الدراسة حيت تنفي فرضية ان المؤهلات الاكاديمية العالية تؤدي الى تبني استراتجيات وسلوكيات رقمنة امنه ما يجعل هدة الممارسات تحديا امنيا شاملا لجميع الفئات .

تخليل الدوافغ الرئيسية وراء الممارسات التخزين الغير الآمن

لفهم الأسباب والدوافع لقيام مستخدمي التطبيقات المصرفية بحفظ البيانات الحساسة بشكل غير أمن تضمن الاستبيان سؤال مباشر لتحديد السبب الرئسي لتخزين البيانات في سجل الاتصال أو في تطبيق معرض الصور تم استخلاص البيانات الموضحة في الجدول ادناة بناء على التحليل الاحصائي الوصفي لاجابات العينة.

جدول (12): التوزيع التكراري للسبب الرئيسي والمحفز للتخزين الغير الأمن للبيانات المصرفية الحساسة

السبب الرئيس	التكرار (Counts)	النسبة المئوية%	النسبة التراكمية%
صعوبة تذكر الارقام الطويلة والمعقدة	64.0	28.8%	28.8%
بطء في عمليات تسجيل الدخول الى التطبيقات المصرفية	35.0	15.8%	44.6%
الخوف من فقدان بيانات الوصول للحساب	51.0	23.0%	67.6%
سهولة النسخ وألصق من جهات الاتصال	72.0	32.4%	100.0%

يتبين من خلال المؤشرات الإحصائية لعينة الفعلية الدراسة (N=222) عن وجود تباين في الدوافع حتث تصدر الدافع "سهولة النسخ والصق:قائمة الدوافع بنسبة (32.4%) ومن ثم الدافع " صعوبة تذكر الأرقام الطويلة والمعقدة" وبنسبة (28.8%) تم جاء في المرتبة الثالثة الدافع "الخوف من فقدان بيانات الوصول للحساب" بنسبة (23%) وأخيرا جاء الدافع "بطء في عمليات تسجيل الدخول الى التطبيقات المصرفية" بنسبة (15%).

ومن خلال تحليل السلوك في مجال الامن السيبراني تتضح نتيجة مفادها ان اغلب المستخدمين يعطون الأولوية للراحة وسرعة الوصول ومرونة الاستخدام على الالتزام بمعاير أمن البيانات وكذلك يفضل العملاء توفير الجهد والوقت من خلال القيام بعمليات تعتمد على النسخ والصق ما يجعلهم عرضة لاحتمالية لمخاطر الاختراق أو هجمات سيبرانية عبر تطبيقات خارجية لديها إمكانية الوصول لجهات الاتصال او وسائط التخزين على هواتفهم الذكية. وتطهر النتائج أيضا ان سياسات الأمان المعقدة التي تفرضها المصارف تشكل عبئا إضافيا ما يدفع العملاء الى البحث عن بدائل لتسهيل معاملاتهم اليومية.

ملخص المناقشة

من خلال عرض النتائج وتحليلها يتبين استنتاجا واصحا يوكد نقاط الضعف المرتبطة بسلوك المستخدمين يمكن تلخيصها في النقاط التالية:

- التفاوت بين الأفعال و النوايا: تتجلى هده الفجوة في التناقص بين سلوك المستخدم الدى يكون حدرا في حماية كلمات المرور (P4) ويتهاونون بشكل خطير مع ارقام بطاقاتهم المصرفية وتفاصيل حساباتهم (P1,P2,P3).
- تتجاوز هذه السلوكيات الفئات الديموغرافية: انعدام الفروق ذات دلالة إحصائية في جميع الاختبارات يؤكد ان التخزين الغير الامن مشكلة سلوكية عامه لا تقتصر على جنس او فئة عمرية او مستوى تعليمي.
- تفضيل سهولة الاستخدام على الامن: أظهرت النتائج ان دافع السهولة والسرعة يتفوق على متطلبات الامن السيبراني ما يوكد حقيقة ان العامل البشرى هو الحلقة الأضعف في نظام الرقمي.
- العلاقة عكسية بين الوعي والممارسة حيث اكد اختبار بيرسون لمعمل الارتباط عن وجود ارتباط عكسي ذي دلالة إحصائية ($r=-0.167, P=0.012$) بين مستوى الوعى الأمني ومعدل الممارسات الخطرة ما يقدم دليلا على ضرورة تبني حملات توعوية شاملة تستهدف جميع العملاء نظرا لانتشار هدة السلوكيات بين جميع الفئات مستخدمه للتطبيقات المصرفية.

الخلاصة

خلصت دراستنا الى ان سلوكيات التخزين الغير الامن للبيانات المصرفية بما في ذلك التخزين في سجل جهات الاتصال او في معرض الصور يمثل تهديدا حقيقيا للأمن السيبراني يؤثر على عدد كبير من مستخدمي التطبيقات المصرفية في القطاع المصرفي الليبي ، وكما خلصت الدراسة على ان أساس المشكلة هي مشكلة سلوكية وليست تقنية ،اظهرت النتائج التي تحصلنا عليها باستخدام برنامج Jamovi لعينه مكونة من 225 مستجيبا ان اكثر من ثلثي العملاء يعرضون بياناتهم المصرفية الحساسة لخطر الاختراق ،كما اتيت الاختبارات ان هدة السلوكيات منتشرة بين جميع الفئات الديموغرافية وكذلك أظهرت ان المستخدمين يلجا الى هذه الممارسات لحاجة وظيفية في ظل غياب بدائل رسمية امنة ضمن التطبيقات المصرفية نفسها . وبناء على ما سبق تبرز رؤية قائمة على المسؤوليات المشتركة بين المؤسسات المصرفية والزبائن حيت يتعين على المصارف الانتقال من نماذج الإنذار الى أسلوب التصميم الوقائي الدى يجعل الامن خيار اكتر سهولة للمستخدم، وكما يتوجب على الجهات التنظيمية مسؤوليه إلزام المؤسسات المصرفية بالالتزام بمعاير امنة وواضحة. وكما يجب على العملاء أدراك ان التخزين البدائي واستخدام الأسماء المستعارة ما هو الا أسلوب ضعيف في مواجهة الخوارزميات الحديثة وتقنيات الاختراق.

وبناء على الاستنتاجات الدراسة نوصي بالتوصيات التالية الى الجهات المعنية:

توصيات للمصارف الليبية

- تطوير خزنة مشفرة للبيانات داخل التطبيقات المصرفية جيت يجب على المصارف إدخال ميزات امان تمكن المستخدم من حفظ بيانات ارقام الحسابات وأرقام البطاقات او حتى صور للبطاقات المصرفية مع اشتراط استخدام المصادقة البيو مترية للوصول الى الخدمات المصرفية ما يلغى الحاجة الى التخزين الغير الرسمي للبيانات الحساسة.
- إطلاق حملات توعوية داخل التطبيق باستخدام الاشعارات الداخلية للتحدير من مخاطر هده السلوكيات مع توفير محتوى تعليمي يشرح خطورة أذونات مزامنة البيانات السحابية.

توصيات للمستخدمين التطبيقات المصرفية

- الامتناع الكامل عن تخزين أي بينات مالية حساسة في قائمة جهات الاتصال الهاتف حتى باستخدام أسماء مستعارة مراجعة اذونات التطبيقات المثبتة على الهواتف ولغاء اذونات الوصول الى جهات الاتصال او ومعرض الصور لأي تطبيق غير ضروري.
- مراجعة اعدادات الخصوصية والأمان وتعطيل خاصية المزامن التلقائية للحسابات المنصات الرقمية المرتبطة بدقة.

توصيات للمصرف المركزي وهيئات الرقابية على المصارف

- اصدار توجيهات تنظيمية تشترط توفير ميزة تخزين بيانات امنة ومحمية ضمن تطبيقات الخدمات المصرفية كشرط أساسي.
- ربط متطلبات ترخيص الأنظمة وتحديتها بمعاير امن السلوك.
- انشاء فرق مختصة لاختبار امن التطبيقات المصرفية في بيئة العمل المحلية وتقيم دوري للثغرات الأمنية وتحسين كفاءة الخدمات البنية التحتية الالكترونية.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

قائمة المراجع:

[1] A. M. A. Khanfar, "ادارة مخاطر التحول الرقمي على أمن المعلومات," pp. 502–522, 2022.

[2] A. A. Alalwan, Y. K. Dwivedi, and N. P. Rana, "Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust," *Int. J. Inf. Manage.*, vol. 37, no. 3, pp. 99–110, 2017.

[3] س. ا. م. السويدي, "تقييم الوعي بأمن المعلومات لدى العاملين في القطاع المصرفي الخاص في مصراتة–ليبيا," and ع. ا. الرواتي *مجلة البحوث الأكاديمية*, vol. 28, no. 1, pp. 18–28, 2024.

[4] L. M. Bishop, P. M. Asquith, and P. L. Morgan, "The employee cybersecurity awareness framework," *Hum. Behav. Emerg. Technol.*, vol. 2025, no. 1, p. 1025045, 2025.

[5] D. Baltuttis, T. Teubner, and M. T. P. Adam, "A typology of cybersecurity behavior among knowledge workers," *Comput. Secur.*, vol. 140, p. 103741, 2024, doi: https://doi.org/10.1016/j.cose.2024.103741.

[6] W. Enck, L. P. Cox, P. Gilbert, and P. Mcdaniel, "TaintDroid : An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones".

[7] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[8] I. Kirlappos, S. Parkin, and A. Sasse, *Learning from "Shadow Security:" Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security*. 2014. doi: 10.14722/usec.2014.23007.

[9] م. ع. ج. ا. ع. م. حميد, "أثر تقنية الذكاء الاصطناعي في تأمين العمليات المالية الرقمية: دراسة حالة من العمليات الرقمية من وجهة نظر الدراسات السابقة," *مجلة العلوم الإنسانية والطبيعية*, vol. 6, no. 7, pp. 483–495, 2025.

[10] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," *arXiv Prepr. arXiv1901.02672*, 2019.

[11] J. Kävrestad, J. Rambusch, and M. Nohlberg, "Design principles for cognitively accessible cybersecurity training," *Comput. Secur.*, vol. 137, p. 103630, 2024, doi: https://doi.org/10.1016/j.cose.2023.103630.

[12] N. Woods and M. Siponen, "How memory anxiety can influence password security behavior," *Comput. Secur.*, vol. 137, p. 103589, 2024, doi: https://doi.org/10.1016/j.cose.2023.103589.

[13] A. Alshamsi, N. Williams, and P. Andras, *The Trade-off Between Usability and Security in the Context of eGovernment: A Mapping Study*. 2016. doi: 10.14236/ewic/HCI2016.36.

[14] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Comput. Secur.*, vol. 34, pp. 47–66, 2013, doi: https://doi.org/10.1016/j.cose.2012.11.004.

[15] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Comput. Surv.*, vol. 48, no. 3, pp. 1–39, 2015.

[16] المركز العربي للأبحاث ودراسة السياسات, "المؤشر العربي 2022: برنامج قياس الرأي العام العربي," الدوحة, 2022. [Online]. Available: www.dohainstitute.org